ABSTRACT

A system and method for encryption and decryption of files. The system and method operate in conjunction with the file system to transparently encrypt and decrypt files in using a public key-private key pair encryption scheme. When a user puts a file in an encrypted directory or encrypts a file, data writes to the disk for that file are encrypted with a random file encryption key generated from a random number and encrypted with the public key of a user and the public key of at least one recovery agent. The encrypted key information is stored with the file, whereby the user or a recovery agent can decrypt the file data using a private key. With a correct private key, encrypted reads are decrypted transparently by the file system and returned to the user. One or more selectable encryption and decryption algorithms may be provided via interchangeable cryptographic modules.